

Claims

1 1. A computer-implemented method for securely transmitting an
2 information package to an addressee via a network, the method comprising the
3 steps of:

4 determining whether the addressee has a public key;

5 in response to the addressee not having a public key:

6 encrypting the package with an escrow encryption key;

7 storing the package in escrow for the addressee;

8 notifying the addressee of the package in escrow; and

9 in response to receiving an acknowledgment from the addressee:

10 issuing new public and private keys to the addressee; and

11 transmitting the package to the addressee via the network.

1 2. The method of claim 1, wherein the step of determining whether
2 the addressee has a public key comprises the sub-step of:

3 checking a public key directory for a public key of the addressee.

1 3. The method of claim 1, further comprising the step of:

2 storing the addressee's new public key in a public key directory.

1 4. The method of claim 1, wherein the encrypting step comprises the
2 sub-steps of:

3 providing an escrow encryption key and an escrow decryption key,
4 wherein the escrow encryption and decryption keys comprise one
5 of symmetric keys and asymmetric keys; and
6 encrypting the package with the escrow encryption key.

1 5. The method of claim 1, wherein the notifying step comprises the
2 sub-step of:

3 sending a notification to the addressee via the network.

1 6. The method of claim 5, wherein the notification comprises one of
2 an e-mail notification, a desktop notification, a voice notification, a pager
3 notification, and a facsimile notification.

1 7. The method of claim 1, further comprising the step of:
2 decrypting the package with an escrow decryption key corresponding to
3 the escrow encryption key.

1 8. The method of claim 1, wherein the escrow encryption key is
2 different from the new public and private keys issued to the addressee.

1 9. The method of claim 1, wherein the acknowledgment from the
2 addressee includes an indication of the addressee's name and e-mail address.

1 10. The method of claim 1, further comprising the step of:
2 in response to an addressee having a public key:
3 encrypting the package with the addressee's public key;
4 storing the package;
5 notifying the addressee of the package;
6 authenticating a user as the addressee; and
7 transmitting the package to the authenticated addressee.

1 11. The method of claim 1, wherein the step of transmitting the
2 package comprises the sub-steps of:
3 authenticating a user as the addressee; and
4 transmitting the package to the authenticated user via the network.

1 12. A computer-implemented method for securely transmitting an
2 information package to an addressee via a network, the method comprising the
3 steps of:
4 determining whether the addressee has a public key;
5 in response to the addressee not having a public key:
6 encrypting the package with an escrow encryption key;

7 storing the package in escrow for the addressee;
8 notifying the addressee of the package in escrow; and
9 in response to receiving an acknowledgment from the addressee:
10 issuing new public and private keys to the addressee;
11 decrypting the package with an escrow decryption key;
12 re-encrypting the package using the addressee's new public
13 key; and
14 transmitting the package to the addressee via the network.

1 13. The method of claim 12, wherein the step of determining whether
2 the addressee has a public key comprises:

3 checking a public key directory for a public key of the addressee.

1 14. The method of claim 12, further comprising:

2 storing the addressee's new public key in a public key directory.

1 15. The method of claim 12, wherein the step of transmitting the
2 package comprises the sub-steps of:

3 authenticating a user as the addressee; and

4 transmitting the package to the authenticated user via the network.

1 16. The method of claim 12, further comprising the step of:

2 decrypting the package using the addressee's new private key.

1 17. A system for securely transmitting an information package to an
2 addressee via a network, the system comprising:
3 a directory interface adapted to check a directory to determine whether
4 the addressee has a public key;
5 an escrow key manager, coupled to the directory interface, adapted to
6 provide an escrow encryption key for encrypting the package;
7 an encryption module, coupled to the escrow key manager, adapted to
8 encrypt the package with the escrow encryption key;
9 a computer-readable medium, coupled to the encryption module, adapted
10 to store the package in escrow for the addressee;
11 a notification module, coupled to the computer-readable medium,
12 adapted to send a notification to the addressee via the network;
13 a key registration module, coupled to the notification module, adapted to
14 issue, in response to the addressee acknowledging the notification,
15 new public and private keys to the addressee; and
16 a transmission module, coupled to the key registration module and to the
17 computer-readable medium, adapted to transmit the package to the
18 addressee via the network.

1 18. The system of claim 17, further comprising:

2 a directory, coupled to the directory interface, adapted to store a public
3 key of at least one addressee.

1 19. The method of claim 18, wherein the key registration module is
2 further adapted to store the addressee's new public key in the directory.

1 20. The system of claim 17, wherein the notification module is adapted
2 to send one of an e-mail notification, a desktop notification, a voice notification, a
3 pager notification, and a facsimile notification.

1 21. The system of claim 17, wherein the escrow key manager is
2 adapted to provide an escrow decryption key, the system further comprising:
3 a decryption module, coupled to the transmission module, adapted to
4 decrypt the package using the escrow decryption key.

1 22. The method of claim 21, wherein the escrow encryption key and
2 the escrow decryption key comprise one of symmetric keys and asymmetric
3 keys.

1 23. The system of claim 17, wherein the directory interface and the
2 encryption module are each adapted to operate within a sending system;
3 wherein the computer-readable medium, the notification module, and the
4 transmission module are each adapted to operate within a server system; and

5 wherein the key registration module and the decryption module are each
6 adapted to operate within a receiving system.

1 24. The system of claim 23, wherein the key registration module is
2 received by the receiving system as an attachment to a notification.

1 25. The system of claim 23, wherein the key registration module is
2 received by the receiving system by following a hyperlink in a notification.

1 26. The system of claim 23, wherein the transmission module within
2 the server system is adapted to transmit the package in escrow to the decryption
3 module within the receiving system; and wherein the decryption module within
4 the receiving system is adapted to receive the package from the transmission
5 module, receive an escrow decryption key from the escrow key manager, and
6 decrypt the package with the escrow decryption key.

1 27. The system of claim 23, wherein the transmission module within
2 the server system is adapted to receive an escrow decryption key from the
3 escrow key manger, decrypt the package in escrow using the escrow decryption
4 key, receive the addressee's public key from a directory, re-encrypt the package
5 using the addressee's public key, and transmit the package to the decryption
6 module within the receiving system; and wherein the decryption module within
7 the receiving system is adapted to receive the package from the transmission

8 module, retrieve the addressee's private key from the key registration module,
9 and decrypt the package using the addressee's private key.

1 28. In a computer-readable medium, a computer program product for
2 securely transmitting an information package to an addressee via a network, the
3 computer-readable medium comprising program code adapted to perform the
4 steps of:

5 determining whether the addressee has a public key;

6 in response to the addressee not having a public key:

7 encrypting the package with an escrow encryption key;

8 storing the package in escrow for the addressee;

9 notifying the addressee of the package in escrow; and

10 in response to receiving an acknowledgment from the addressee:

11 issuing new public and private keys to the addressee; and

12 transmitting the package to the addressee via the network.